UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,075	09/19/2005	Youdai Watanabe	2611.0233PUS1	2661

2292 7590 12/09/2008
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
SU, SARAH	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
12/09/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/528,075	WATANABE ET AL.	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☒ Claim(s) *13* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 September 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Amendment A, received on 18 September 2008, has been entered into record. In this amendment, claims 1-24 have been amended.

2. Claims 1-24 are presented for examination.

Response to Arguments

3. Applicant's arguments, filed 18 September 2008, with respect to the rejection(s) of claim(s) 1, 3-6, 9, 11-14, 17, 19-22 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Bennett et al. ("Quantum Cryptography: Public Key Distribution and Coin Tossing" 1984 and Bennett hereinafter).

Information Disclosure Statement

4. The information disclosure statement filed 17 March 2005 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because it does not include a legible copy and English translation of the cited Uchiyama reference. It has been placed in the application file, but the information referred to therein has not been considered as to the merits.

Drawings

5. The drawings were received on 18 September 2008. These drawings are acceptable.

Claim Objections

6. Claim 13 is objected to because of the following informalities: in claim 13, line 7: "a part of pieces of the common information" is unclear if it relates to "a part of pieces of the common information" (claim 9, lines 15-16).

Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claims 1, 9, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamazaki (Institute of Electronics, Information and Communication Engineers Society Conference 2001) in view of Bennett.

As to claims 1, 9, and 17, Yamazaki discloses a system and method for error correcting codes for quantum key distribution, the system and method having:

a check matrix creation step of each of the first communication apparatus and the second communication apparatus creating the same parity check matrices H(n×k) (page 5, lines 10-12)**;**

a random number generation step of the first communication apparatus generating a random number sequence (transmission data) and randomly determining a predetermined transmission code (base) by the first communication apparatus, and the second communication apparatus randomly determining a predetermined reception code (base) (page 2, lines 14-16)**;**

a data deletion step of each of the first communication apparatus and the second communication apparatus deciding whether the measuring has been performed with an appropriate measuring apparatus, saving the reception data of n bits if the measuring has been performed with the appropriate measuring apparatus and transmission data that corresponds

to the reception data, and discarding other pieces of the data (page 2, lines 17-20);

an error correction information notification step of the first communication apparatus notifying the second communication apparatus through a public communication path of error correction information of k bits based on the parity check matrix H and the transmission data of n bits (page 4, lines 20-24; page 5, lines 21-24);

an error correction step of the second communication apparatus correcting the error of the reception data based on the parity check matrix H, the reception data of n bits, and the error correction information (page 5, lines 1-6).

Yamazaki does not disclose:

a photon transmission step of the first communication apparatus transmitting a photon onto the quantum communication path while the photon is in a quantum state specified by a combination of the transmission data and the transmission code;

a photon reception step of the second communication apparatus measuring the photon transmitted on the quantum communication path to obtain reception data specified by the combination of the reception code and measurement result;

a cryptographic key creation step of each of the first communication apparatus and the second communication apparatus discarding a part of

pieces of the common information (n) after correction according to public error correction information, creating a cryptographic key using information that has remained after discarding, and setting the cryptographic key as a common key which is shared between first communication apparatus and the second communication apparatus.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Yamazaki, as evidenced by Bennett. Bennett discloses a system and method for public key distribution, the system and method having:

a photon transmission step of the first communication apparatus transmitting a photon onto the quantum communication path while the photon is in a quantum state specified by a combination of the transmission data and the transmission code (col. 5, lines 4-8);

a photon reception step of the second communication apparatus measuring the photon transmitted on the quantum communication path to obtain reception data specified by the combination of the reception code and measurement result (col. 5, lines 10-13);

a cryptographic key creation step of each of the first communication apparatus and the second communication apparatus discarding a part of pieces of the common information after correction according to public error correction information, creating a cryptographic key using information that has remained after discarding, and setting the

cryptographic key as a common key which is shared between first communication apparatus and the second communication apparatus (col. 4, lines 53-58; col. 5, lines 8-17).

Given the teaching of Bennett, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Yamazaki with the teachings of Bennett by transmitting photons and creating a shared key. Bennett recites motivation by disclosing that transmitting polarized photons provides for a communications channel on which it is impossible to eavesdrop without a high probability of disturbing the transmission (col. 1, lines 1-8) and that the need for immunity to active eavesdropping is reduced if transmitters and receivers are using a key (col. 5, lines 40-43). It is obvious that the teachings of Bennett would have improved the teachings of Yamazaki by providing for photon transmission and cryptographic key creation in order to reduce the probability of successful eavesdropping and to reduce the need for protection against active eavesdropping.

10. Claims 2, 7, 10, 15, 18, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamazaki in view of Bennett as applied to claims 1, 9, and 17 above, and further in view of Kou et al. (IEEE Globecom and Kou hereinafter) and Chung et al. (IEEE Transactions on Information Theory and Chung hereinafter).

As to claims 2, 10, and 18, Yamazaki in view of Bennett does not disclose:

weight searching step of using finite affine geometry as a basic matrix and searching optimum row and column weight distributions of the parity check matrix by performing optimization of Gaussian approximation,

dividing step of dividing randomly the row and column weights of the finite affine geometry based on the optimum weight distribution by a predetermined procedure, and creating the parity check matrix H of a low-density parity check code in which both the row and column weights or one of the row and column weights is not uniform.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Yamazaki in view of Bennett, as evidenced by Chung.

Chung discloses a method for sum-product decoding of low-density parity check codes using a Gaussian approximation, the method having:

weight searching step of using finite affine geometry as a basic matrix and searching optimum row and column weight distributions of the parity check matrix by performing optimization of Gaussian approximation (col. 17, lines 2-3; col. 18, lines 28-32) in order to provide for a simple way to estimate thresholds for low density parity check codes, as recited in Chung (col. 2, lines 38-43).

Yamazaki in view of Bennett and Chung does not disclose:

dividing step of dividing randomly the row and column weights of the finite affine geometry based on the optimum weight distribution by a

predetermined procedure, and creating the parity check matrix H of a low-density parity check code in which both the row and column weights or one of the row and column weights is not uniform.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Yamazaki in view of Bennett and Chung, as evidenced by Kou.

Kou discloses a system and method for low density parity check codes based on finite geometries, the system and method having:

dividing step of dividing randomly the row and column weights of the finite affine geometry based on the optimum weight distribution by a predetermined procedure, and creating the parity check matrix H of a low-density parity check code in which both the row and column weights or one of the row and column weights is not uniform (col. 7, lines 37-41; col. 8, lines 1-8).

Given the teaching of Kou, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Yamazaki in view of Bennett and Chung with the teachings of Kou by randomly splitting the row and column weights. Kou recites motivation by disclosing that the parity check code can be extended by splitting the columns which results in a smaller density new code (col. 7, lines 27-31). It is obvious that the teachings of Kou would have improved the teachings of Yamazaki in view of Bennett and Chung by

splitting the rows and columns in order to produce new check codes with smaller densities.

As to claims 7, 15 and 23, Yamazaki in view of Bennett and Chung do not disclose:

> **performing random permutation to the column of the parity check matrix H, selecting specific "1" in the first column of finite affine geometry AG(2,2^S) of a creation element of the parity check matrix H, exchanges a position of "1" through the public communication path, specifying the position (column) after the division corresponding to "1" from the parity check matrix after the random permutation and the position (column) after the division corresponding to "1" in each cyclically shifted column, and discarding the part of pieces of the common information corresponding to the specified position (column).**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Yamazaki in view of Bennett and Chung, as evidenced by Kou.

Kou discloses:

> **performing random permutation to the column of the parity check matrix H, selecting specific "1" in the first column of finite affine geometry AG(2,2^S) of a creation element of the parity check matrix H, exchanges a position of "1" through the public communication path, specifying the position (column) after the division corresponding to "1" from the parity**

check matrix after the random permutation and the position (column) after the division corresponding to "1" in each cyclically shifted column, and discarding the part of pieces of the common information corresponding to the specified position (column) (col. 7, lines 37-41; col. 8, lines 1-8).

Given the teaching of Kou, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Yamazaki in view of Bennett and Chung with the teachings of Kou by changing the columns of a check matrix. Please refer to the motivation recited above in respect to claims 2, 10 and 18 as to why it is obvious to apply the teachings of Kou to the teachings of Yamazaki in view of Bennett and Chung.

11. Claims 8, 16, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamazaki in view of Bennett, Chung and Kou, as applied to claims 7, 15, and 23 above, and further in view of Wu et al. ("Generalised inverses in public key cryptosystem design" 1998 and Wu hereinafter).

As to claims 8, 16 and 24, Yamazaki in view of Bennett, Chung, and Kou does not disclose:

one of the communication apparatuses, out of the first communication apparatus and the second communication apparatus, creating a nonsingular random matrix R((n-k)×(n-k)) to act on the cryptographic key after discarding the part of pieces of the common

information and informing the nonsingular random matrix R to other one of the communication apparatuses through the public communication path,

the first communication apparatus and the second communication apparatus using the nonsingular random matrix R to create the cryptographic key.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Yamazaki in view of Bennett, Chung, and Kou, as evidenced by Wu.

Wu discloses a system and method for generalized inverses in a public key cryptosystem, the system and method having:

one of the communication apparatuses, out of the first communication apparatus and the second communication apparatus, creating a nonsingular random matrix R((n-k)×(n-k)) to act on the cryptographic key after discarding the part of pieces of the common information and informing the nonsingular random matrix R to other one of the communication apparatuses through the public communication path (page 323, col. 1, lines 26-28),

the first communication apparatus and the second communication apparatus using the nonsingular random matrix R to create the cryptographic key (page 321, col. 2, lines 11-13).

Given the teaching of Wu, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying

the teachings of Yamazaki in view of Bennett, Chung, and Kou with the teachings of Wu by using a random matrix to create a cryptographic key. Wu recites motivation by disclosing that using generalized matrices provides for a smaller key size with the same level of security (Abstract, lines 9-16). It is obvious that the teachings of Wu would have improved the teachings of Yamazaki in view of Bennett, Chung, and Kou by using a random matrix to create a cryptographic key in order to provide for the same of level of security while using a smaller key.

12. Claims 3-6, 11-14, and 19-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamazaki in view of Bennett as applied to claims 1, 9, and 17 above, and further in view of Wu.

As to claims 3, 11, and 19, Yamazaki, combined with Bennett, discloses:

> **wherein the check matrix creation step includes creating an inverse matrix G^{-1} (n×(n-k)), which satisfies $G^{-1} \cdot G = I$ (unit matrix), from a creation matrix G((n-k)×n) satisfying "HG=0"** (page 4, lines 10-11; page 5, line 10).

Yamazaki in view of Bennett does not disclose:

> **the cryptographic key creation step includes discarding the part of pieces of the common information by the inverse matrix G^{-1}.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Yamazaki in view of Bennett, as evidenced by Wu.

Wu discloses:

the cryptographic key creation step includes discarding the part of pieces of the common information by the inverse matrix G^{-1} (page 323, col. 1, lines 22-36).

Given the teaching of Wu, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Yamazaki in view of Bennett with the teachings of Wu by creating a key using an inverse matrix. Please refer to the motivation recited above in respect to claims 8, 16, and 24 as to why it is obvious to apply the teachings of Wu to the teachings of Yamazaki in view of Bennett.

As to claims 5, 13, and 21, Yamazaki, combined with Bennett, discloses:

wherein the check matrix creation step includes creating a mapping F to map an n-dimensional vector (i.e. code) **to an m-dimensional vector (m ≤ n-k)** (i.e. block)**, the mapping F being one in which the number of elements of a reverse image $(F \cdot G)^{-1}$ (v) in a composition mapping FG of the mapping F and the creation matrix G satisfying "HG=0" is independent of an arbitrary m-dimensional vector v and is constant (2^{n-k-m})** (page 3, lines 12-14, 19-21; page 4, lines 8-11)**.**

Yamazaki in view of Bennett does not disclose:

the cryptographic key creation step includes discarding a part of pieces of the common information (n) by the mapping F.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Yamazaki in view of Bennett, as evidenced by Wu.

Wu discloses:

> **the cryptographic key creation step includes discarding the part of pieces of the common information by the mapping F** (page 323, col. 1, lines 22-36).

Given the teaching of Wu, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Yamazaki in view of Bennett with the teachings of Wu by creating the key with a mapping. Please refer to the motivation recited above in respect to claims 3, 11, and 19 as to why it is obvious to apply the teachings of Wu to the teachings of Yamazaki in view of Bennett.

As to claims 4, 6, 12, 14, 20, and 22, Yamazaki in view of Bennett does not disclose:

> **one of the communication apparatuses, out of the first communication apparatus and the second communication apparatus, creating a nonsingular random matrix R((n-k)×(n-k)) to act on the cryptographic key after discarding the part of pieces of the common information and informing the nonsingular random matrix R to other one of the communication apparatuses through the public communication path**,

the first communication apparatus and the second communication apparatus using the nonsingular random matrix R to create the cryptographic key.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Yamazaki in view of Bennett, as evidenced by Wu.

Wu discloses a system and method for generalized inverses in a public key cryptosystem, the system and method having:

one of the communication apparatuses, out of the first communication apparatus and the second communication apparatus, creating a nonsingular random matrix R((n-k)×(n-k)) to act on the cryptographic key after discarding the part of pieces of the common information and informing the nonsingular random matrix R to other one of the communication apparatuses through the public communication path (page 323, col. 1, lines 26-28),

the first communication apparatus and the second communication apparatus using the nonsingular random matrix R to create the cryptographic key (page 321, col. 2, lines 11-13).

Given the teaching of Wu, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Yamazaki in view of Bennett with the teachings of Wu by using a random matrix to create a cryptographic key. Please refer to the motivation recited

above in respect to claims 8, 16, and 24 as to why it is obvious to apply the teachings of Wu to the teachings of Yamazaki in view of Bennett.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2431

/Christopher A. Revak/

Primary Examiner, Art Unit 2431